



Sichere Mobilitätslösung von Aruba für vorhandene WLANs

Zahlreiche zukunftsorientierte Organisationen sind sich seit langem der Vorteile der WLAN-Technologie (Wireless-LAN) bewusst. Sie haben diese Technologie implementiert, um die Mitarbeiterproduktivität zu verbessern, neue Anwendungen bereitzustellen und die Netzwerkmobilität zu ermöglichen. Damals bestand die aktuelle WLAN-Technik aus eigenständigen („Thick“) Access-Points und dem WEP-Verschlüsselungsprotokoll. Heute gelten diese Technologien im besten Fall als umständlich und im schlimmsten Fall als gefährlich, und trotzdem haben viele Organisationen in beträchtlichem Umfang in die Technologie investiert und können sich keine umfassende Aktualisierung leisten. Aruba Networks ermöglicht diesen Organisationen die Aktualisierung ihrer vorhandenen WLAN-Access-Points zur Bereitstellung eines modernen benutzerzentrischen Netzwerks.

Erforderliche Aktualisierung von WLANs

FEHLENDE MOBILITÄT

Vorhandene APs sind mit VLANs und IP-Subnetzen verankert, weshalb auch Wireless-Clients mit diesen VLANs verankert sind. Greift ein Client auf einen AP zu, der mit einem anderen VLAN verbunden ist, erfolgt die Kommunikation nicht nahtlos. Clients müssen eine neue IP-Adresse anfordern, und Sitzungen müssen neu gestartet werden.

LÜCKEN BEI DER WLAN-SICHERHEIT

Viele ältere APs unterstützen nur WEP und können nicht zur Unterstützung von WPA2, dem aktuellen Standard für die Wireless-Sicherheit, aktualisiert werden. Aus diesem Grund ist die Organisation einem hohen Risiko ausgesetzt, da sich WEP leicht knacken lässt. Vorhandene WLANs erlauben allen Benutzern den Gesamtzugriff – nachdem ein Benutzer im Netzwerk angemeldet ist, kann er auf alles zugreifen. Daher

ist die Gewährleistung des sicheren Gastzugriffs unmöglich. Im Netzwerk entstehen Lücken, durch die einfache Geräte wie drahtlose Strichcodeleser umfassende Berechtigungen erhalten.

FEHLENDE WLAN-TRANSPARENZ

In vorhandenen WLANs ist entweder keine oder nur beschränkte Transparenz in der RF-Domäne vorhanden. Manuelle Prozesse wie die Fehlerbehebung, Rogue-AP-Erkennung und -Ortung und die Erkennung von Angriffen erfordern ausführlich WLAN-Kenntnis.

UMSTÄNDLICHE FEHLERBEHEBUNG

Ist ein vorhandener AP aus dem Netzwerk nicht erreichbar, greifen die Administratoren oft zur Leiter und klettern über die abgehangene Decke, um den Fehler zu finden. Diese Vorgehensweise ist zeitaufwendig und teuer.

So sichert und mobilisiert Aruba vorhandene WLANs

Durch die Installation eines Aruba Mobility Controllers im Netzwerk und die physikalische oder logische Verbindung vorhandener APs mit dem Controller kommen die vorhandenen APs in den Genuss zahlreicher Vorteile eines modernen zentralisierten WLAN.

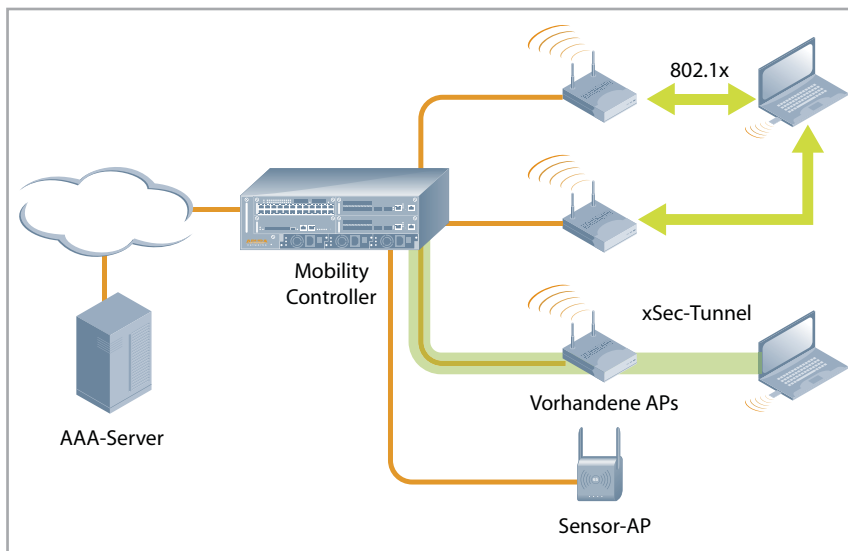
NAHTLOSES ROAMING

Das Proxy-DHCP von Aruba ermöglicht unabhängig vom VLAN, mit dem ein AP physikalisch verbunden ist, das nahtlose Roaming. Bei der ersten Verbindungsherstellung des Client mit dem Netzwerk wird

Vorteile:

- Sofortige höhere WLAN-Sicherheit, ohne APs zu ersetzen
- Problemloses Roaming zwischen VLANs
- Höhere Gesamtsicherheit mittels Wireless Intrusion Protection
- Bessere ichtliniendurchsetzung mittels Stateful-Firewall von Aruba
- Einfacher Migrationspfad vom vorhandenen WLAN zum modernen zentralisierten WLAN

Sicherere Mobilität für vorhandene WLANs



ihm gemäß normaler Regeln eine IP-Adresse zugewiesen (das VLAN, in dem sich der AP befindet). Beim Roaming des Client wird bei jedem Zugriff auf einen neuen AP vom DHCP-Server eine neue IP-Adresse angefordert. Der Mobility Controller empfängt die DHCP-Anforderung und reagiert darauf, indem er dem Client mitteilt, dieselbe IP-Adresse zu verwenden. Auf diese Weise behält der Client sein konsistentes Bild vom Netzwerk bei, während das Netzwerk sein konsistentes Bild vom Client behält. Somit kann ein Client im gesamten Netzwerk, innerhalb und zwischen VLANs roamen, ohne dass Sitzungen zurückgesetzt werden.

STATEFUL 802.1X

Mithilfe von Stateful 802.1x erfährt der Mobility Controller die Identität und Rolle eines Benutzers, der mit einem Drittanbieter-AP verbunden ist. Sendet ein 802.1x-fähiger Access-Point eine RADIUS-Anforderung an den AAA-Server, prüft der Mobility Controller diese Anfrage und die zugehörige Antwort, um den Authentifizierungsstatus des Benutzers zu erfahren. Anschließend wird die auf der Identität basierende Sicherheit über die Policy Enforcement Firewall angewendet.

POLICY ENFORCEMENT FIREWALL (FIREWALL ZUR RICHTLINIEN-DURCHSETZUNG)

Der Mobility Controller kann mithilfe der ICSA-zertifizierten Policy Enforcement Firewall (PEF) von

Aruba für Benutzer von Drittanbieter-APs die auf der Identität basierende Zugriffskontrolle durchsetzen. Auf diese Weise können Benutzern auf der Gruppenmitgliedschaft basierende Rollen mit unterschiedlichen Zugriffsrechten zugewiesen werden. Unter Verwendung der PEF kann Benutzern mit Laptops der Vollzugriff und Geräten wie Strichcodelesern der eingeschränkte Zugriff zugewiesen werden, auch wenn beide Geräte dieselbe SSID verwenden. Außerdem kann der Gastzugriff nur auf das Internet beschränkt werden, während Subunternehmer beschränkte Rechte für das interne Netzwerk erhalten.

SERIAL- UND POWER-OVER-ETHERNET

Sind Drittanbieter-APs mit einem Mobility Controller direkt verbunden, werden vom Mobility Controller Power-over-Ethernet und Serial-over-Ethernet (SOE) bereitgestellt. Bei Verwendung von SOE mit dem entsprechenden Splitter kann die Konsolenverbindung zum AP mit dem integrierten Terminalserver des Mobility Controllers hergestellt werden, indem über unbelegte Adern in standardmäßigen Twisted-Pair-Kabeln eine serielle RS-232-Verbindung hergestellt wird. Administratoren brauchen dann nicht mehr auf Leitern steigen und zur Fehlerbehebung Konsolenports mit APs zu verbinden. Administratoren müssen lediglich den Mobility Controller über Telnet oder SSH verbinden und können sofort auf den Drittanbieter-AP zugreifen.

Sicherere Mobilität für vorhandene WLANs

XSEC LAYER-2 VPN

Einige vorhandene APs können nicht zur Unterstützung moderner Sicherheitsstandards wie WPA oder WPA2 aktualisiert werden. xSec von Aruba ermöglicht die vollständige Umgehung der Sicherheit dieser APs, während die Vorteile von WPA2 mit AES-Verschlüsselung weiterhin bereitgestellt werden. Mit der xSec-Clientsoftware wird über die Drahtlosverbindung zu einem Aruba Mobility Controller ein sicherer Tunnel gebildet. Während der AP im „offenen“ Modus betrieben werden kann, wird der gesamte über den AP geleitete Datenverkehr wie beim WPA2 authentifiziert und verschlüsselt. Die Clientsoftware ist für verschiedene gängige Betriebssysteme erhältlich.

RF-TRANSPARENZ

Werden dem Netzwerk ein paar Aruba-APs als Überwachungsgeräte hinzugefügt, erhält der

Netzwerkadministrator RF-Transparenz und kann Aktivität, Störungen und Fehler sehen. Zur Fehlerbehebung können Live-Remotepakete erfasst und an den Aruba Enterprise Analyzer geleitet werden.

WIRELESS INTRUSION PREVENTION

Zur Verbesserung der Wireless-Sicherheit bietet Aruba das in jeden Mobility Controller integrierte Wireless Intrusion Prevention-Modul. Dieses System überwacht sowohl Aruba-APs als auch Drittanbieter-APs und kann verschiedene WLAN-Anfälligkeiten und Attacken auf WLANs wie Rogue-APs, Bridging-Client-Geräte und Denial-of-Service-Attacken erkennen. Weitere Fähigkeiten wie die Ereigniskorrelation und die erweiterte Visualisierung bietet Aruba in der eigenständigen Softwareanwendung RFprotect™, die in die als Sensoren agierenden Wireless-APs von Aruba integriert wird.



WWW.ARUBANETWORKS.COM

1322 Crossman Avenue. Sunnyvale, CA 94089 (USA) | Tel. +1 408.227.4500 | Fax. +1 408.227.4550